HACKER JOURNAL

Anno 1 - N. 18
30 Gennaio / 12 Febbraio 2002

Boss: theguilty@hackerjournal.it

Editor: grAnd@hackerjournal.it,

Graphic designer: Karin Harrop

Contributors: Bismark.it, CAT4R4TTA, Roberto "decOder" Enea, Lele-Altos.tk, KoRn, Antonio Benfante, Paola Tigrino

Publishing company
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing
Stige (Torino)

Distributore
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81-
Tel. 06.33455.1 r.a.
20134 Milano, via Cavriana, 14
Tel. 02.75417.1 r.a.
Pubblicazione quattordicinale registrata al Tribunale di Milano il 25/03/02 con il numero 190.
Direttore responsabile Luca Sprea

HJ: INTASATE LE NOSTRE CASELLE

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati.

redazione@hackerjournal.it

hack·er (hăk'∂r)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

BENTORNATO A CASA, KEVIN



Il 21 gennaio scorso è finalmente scaduto per Kevin Mitnick il divieto a utilizzare i computer e ad accedere a Internet. Quando il "condor" (questo è il suo nickname) si era collegato l'ultima volta a Internet, Windows 95 era ancora in fase beta, e la comunità della Rete era formata da circa 30 milioni di persone, più o meno quanti ce ne sono oggi nella sola Germania.

Fino alla settimana scorsa, Kevin ha potuto ricevere posta elettronica solo attraverso una persona che la scaricava per lui e la stampava, non ha potuto usare il Web, non ha potuto usare un computer per scrivere il suo libro (di cui abbiamo pubblicato sul numero 17 il capitolo censurato). Addirittura, per un periodo più ristretto di tempo, gli è anche stato impedito addirittura di scrivere o parlare di computer o del suo caso giudiziario. Questo divieto era una delle condizioni imposte dalla corte per ottenere la libertà su cauzione.

Oh, chiariamoci: Kevin Mitnick ha commesso dei reati, ed è giusto che sia stato punito. Il punto è che a causa di una corte federale alla ricerca della notorietà che i media hanno dato al "caso Mitnick", Kevin ha dovuto subire un processo dalla legittimità molto dubbia, e gli è stata inflitta una pena sproporzionata alla gravità dei reati commessi. Soprattutto se si considera che è stato privato della possibilità di lavorare nel campo che gli è più congeniale.

Negli Stati Uniti fortunatamente si sta discutendo molto sulla legittimità e l'opportunità di misure restrittive come quelle inflitte a Mitnick. Alcuni tribunali sostengono che si tratti di un deterrente necessario, ma secondo la corte di New York sarebbe una misura troppo drastica, visto che ormai Internet è per molti uno strumento indispensabile per l'esistenza quotidiana, come il telefono, la televisione o i giornali. Speriamo quindi che Kevin possa essere l'ultima persona condannata a vivere offline.

grand@hackerjournal.it

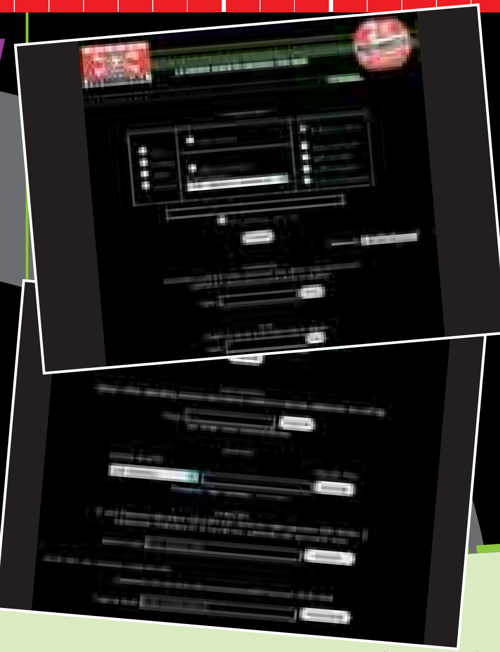
HACKER JOURNAL

Saremo di nuovo in edicola Giovedì 30 Gennaio!

IL CORAGGIO DI OSARE: INDIPENDENTI DA TUTTI

Hackerjournal.it, il muro per i tuoi graffiti digitali

www.hackerjournal.it



Il sito di HJ è in perenne cambiamento, e qualche maligno sostiene che è proprio per quello che ogni tanto qualcosa finisce fuori posto e non funziona correttamente. Per un paio di giorni, le password del n. 17 per la Secret Zone, l'area riservata dove trovate gli arretrati della rivista in formato Pdf e tanti altri servizi utili, non hanno funzionato correttamente. In compenso, il fido Bismark ha aggiunto una pagina con svariati strumenti per la diagnostica e il reperimento di informazioni su reti e server.
La trovate su: www.hackerjournal.it/php-bin/gof.php?go=networktools

SONDAGGIO: PRIVACY O SICUREZZA?

La contrapposizione tra sicurezza e privacy è uno degli argomenti ricorrenti di questo periodo: meglio permettere intercettazioni e schedature di massa, e identificare qualche terrorista, oppure non avere il fiato sul collo del governo, ma identificare molti meno sospetti? Sul versante informatico, meglio impedire connessioni e mail anonime, tracciare tutto il tracciabile e loggare tutto il loggabile, oppure adottare un atteggiamento più libertario ma subire virus, trojan, spam e worm? Come ci aspettavamo, i visitatori di HackerJournal.it scelgono la privacy (probabilmente perché preferiscono pensare in prima persona alla propria sicurezza), ma francamente non pensavamo che il divario tra le due opzioni sarebbe stato così sottile. Segno dei tempi?

Nuova password!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troverete informazioni e strumenti interessanti. Con alcuni browser, potrebbe capitare di dover inserire due volte gli stessi codici. Non fermatevi al primo tentativo.

user: maes3
pass: ge9si

Dai bit alla carta


www.wolfoatkar.com (Wolf Oatkar)

ECCO ALCUNI DEI VOSTRI SITI. Se volete comparire in questo spazio, scrivete a: redazione@hackerjournal.it

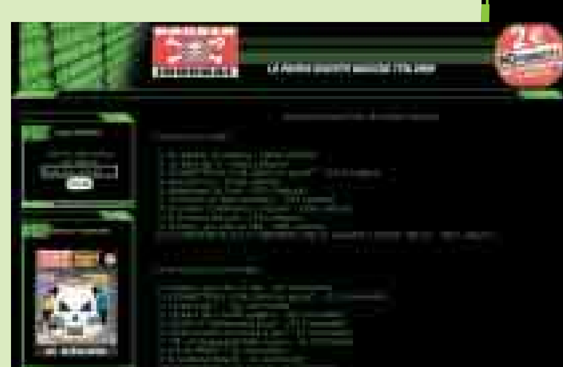
www.hackerdark.it (Legoland),
www.iguanacrew.da.ru (Master Iguana),
www.wmachine.com (Biciuz),
http://zerocoolhak.da.ru (Neo),
www.italianextra.tk (ErEiSeR),
www.hackerunited.com (Giovo).

I MIGLIORI ARTICOLI

Ecco una classifica degli articoli più letti sul sito di HJ. Volevamo anche premiare gli autori in qualche modo (che so, una t-shirt o un cappellino) ma - ahimè - la maggior parte degli articoli ha lo stesso autore: anonymous. Se volete sperare di guadagnarvi qualche gadget, dovete prima registrarvi!

1. Il registro di sistema	(2869 visite)
2. Le basi del C	(1470 visite)
3. Connettersi con Linux by gaxt87	(1335 visite)
4. Netrunner 16 Out!	(1220 visite)
5. anonymous	(1195 visite)
6. Try2hack la sfida continua	(898 visite)
7. Il Sistema Binario	(872 visite)
8. Hacker, uno stile di vita	(800 visite)
9. Buffer Overflow nel Point-to-Point Tunneling Protocol	(789 visite)
10. L'informatica e il fenomeno degli hacker: i nuovi "eroi"	(765 visite)

✪ Oltre alla classifica generale, vogliamo segnalarvi alcuni interessanti articoli che, per la loro novità o perché trattano di argomenti specifici, ancora non hanno accumulato molti lettori. Si tratta degli articoli "TCPDump" di [F]ro[D]o, di "Buco nel gioiello di casa Apple: Jaguar Server" di sp00fffff, e di "Il sistema binario", di qualcuno che non ha voluto dirci il suo nome.



STAMPA LIBERA
NO PUBBLICITÀ
SOLO INFORMAZIONI E ARTICOLI

mailto:
redazione@hackerjournal.it

TROJAN DIABOLICO

Salve a tutti, sono Saty_VII e volevo avere informazioni su un trojan che utilizza la porta di default: 666. Siccome ne sono infetto volevo chiarimenti su come rimuovere questo trojan.

saty_VII

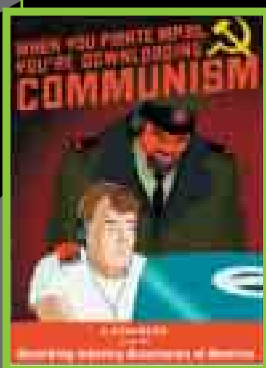
Sul nostro sito, e precisamente all'indirizzowww.hackerjournal.it/php-bin/go.php?go=dbtroyan, trovi una lista dei più diffusi trojan e delle relative porte utilizzate. Per la 666 abbiamo i seguenti candidati: Attack FTP, Back Construction, Cain & Abel, Satanz Backdoor, ServeU, Shadow Phyre. A questi possiamo aggiungere anche Unicorn e yoyo.
Le istruzioni per identificarli e rimuoverli variano a seconda del tipo, quindi non possiamo aiutarti ulteriormente.

SOFTWARE SOSPETTO

Mi sono iscritto a www.freedivx.it ed ho trovato una nuova(?) versione di FlaskMPEG (versione esperta e superlusso, mi pare Xsi, che non si trova sul sito ufficiale del software. Potreste controllare se è una vera versione? PestPatrol mi dice che contiene un pest (almeno uno spyware).

a3tius

Esistono effettivamente le versioni Xis e Xis Expert Edition, ottenute dalla modifica di FlaskMPEG, ma non compaiono sul sito ufficiale di FlaskMPEG. Questo non è un fatto strano, perché FlaskMpeg è un programma libero e open source: chiunque può fare modifiche e distribuire i programmi derivati (a patto di continuare a rispettare la licenza Gnu).
In realtà, da quanto si capisce dal sito ufficiale della versione modificata (www.mp3guest.com/xmpeg_index.asp), il nome è stato cambiato in XMPEG, e sembrerebbe una cosa seria. La versione che hai scaricato tu però potrebbe essere stata ulteriormente modificata, se PestPatrol ti da quell'avviso. Ti consigliamo di scaricare nuovamente XMPEG dal sito citato in precedenza, e di farlo analizzare da PestPatrol.



UNO SPETTRO SI AGGIRA PER LA RETE...

Scrivo di informatica su un sito (palamito.it) e solitamente allego un immagine al mio articolo, il punto è che girando in cerca di immagini sulla Riaa con Google mi è venuta fuori questa.
Da parte di questa associazione mi sembra veramente una cosa vergognosa, e non perché siamo paragonati a dei comunisti ma perché oltre a farne una cosa collettiva utilizza questo termine in modo dispregiativo. Sembra un po' la lotta tra Microsoft e Linux... A voi l'opinione.

Mr_F3d4

Che vuoi commentare... evidentemente le loro strategie di comunicazione sono sono rimaste alla propaganda del dopoguerra.

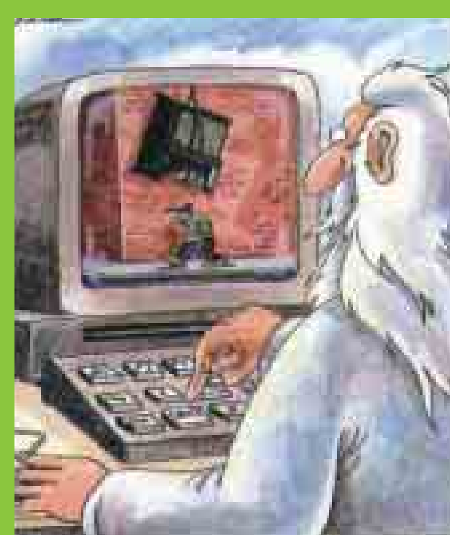
ANCORA SUI VIDEO PER PLAYSTATION

ciao volevo chiedervi un aiuto... come faccio a portare i film in dvd su cd, per vederli con la psx2.
Io ho usato Easydvx (usando la vostra guida trovata sul N°4 di HJ), ma quello vq bene per pc, ma per vederli sulla psx2 come si fa?
Poi, dove posso trovare gratis un dvd player per pc???? io uso power dvd 4, ma è gratuito solo per 30 giorni. Sapete dove poter trovarne uno simile gratis?



Abbiamo descritto come realizzare dei CD con video per Playstation 1 sui numeri 10 e 14, ma non riuscirai mai a far stare un film intero su un CD per PSX con quei sistemi. Se però hai una PlayStation 2, ci sono buone notizie: esiste un software chiamato PS2Reality Mediaplayer che promette di riprodurre vari formati video, tra cui i filmati codificati con DivX. Non siamo ancora riusciti a provarlo, ma sul forum molti utenti sono riusciti a farlo funzionare, anche se con qualche fatica. Trovi tutto sul sito www.ps2reality.net. È in spagnolo, ma alcune sezioni del forum sono in lingua inglese.
Per quanto riguarda i DVD Player gratuiti per PC, uno dei più conosciuti è Video Lan Client (www.videolan.org), che esiste per Windows, vari Unix, Mac OS X e persino BeOS. Ne trovi altri anche su www.webattack.com/freeware/gmm/fwdvd.shtml.

☺ Tech Humor ☺



"Dio, al suo computer, qualche milione di anni dopo aver digitato PKUNZIP UNIVERSE."

TRY2HACK E P2P

Sono ancora un 9llino che non riesce a superare il 2°livello di try2hack... ed è proprio di questo che volevo parlarvi. Ho superato il primo livello con facilità,ma il secondo non sono riuscito a passarlo. Ho capito che serve Macromedia Flash MX, ma ho già sprecato i primi 30 giorni di uso.
Un altra piccola cosa: mi potreste indicare il migliore programma di condivisione file per scaricare divx? Uso attualmente WinMX ma cercavo qualcuno più veloce!
W l'Internet libero!
quasarlibero

Non è necessario avere Flash, né alcun programma a pagamento per superare i livelli di Try2Hack! Ingegnati un po' e prova a guardare il contenuto del file del filmato Flash in altri modi (per esempio con Blocco Note).



WinMx è veloce, se si collega ai server giusti. Prova a utilizzarlo in modalità OpenNap (dalla schermata iniziale), e ad aggiungere dei server affidabili e vicini a te (ne trovi una lista su http://www.napigator.com/servers).

NON È UNA CRITICA!

Premetto che siete una delle mie riviste preferite. Detto ciò, siccome sono abbastanza scrupoloso, mi sono sempre chiesto il perché di alcune cose. So che voi non potete mettervi a rischio svelando i segreti o gli eventuali programmi che un hacker potrebbe usare (anche se non ha bisogno!!!), pena la chiusura e/o l'arresto dei redattori eccetera, ma perché il nome della rivista, allora, ILLUDE tanti ragazzi (e ragazzini!) che aspirano (come me!) a capirne di più sull'argomento? Non che a me non vada bene, anche se mi piacerebbe saperne di più sulle tecniche di hackeraggio (alcune le conosco...), ma mi sembra un po' controsenso chiamare una rivista con un nome e poi non POTERNE parlare liberamente. Ok, Ok... la legge italiana (o forse mondiale?) su tale argomento fa schifo sotto ogni punto di vista. Per dire la verità, mi sono illuso anche io le prime volte che ho comprato la rivista (tanto vero che dal giornalaio a casa mia la nascondevo sotto il giubbotto!). Ecco, mi sono sfogato, ve l'ho detto! Non penso di essere stato offensivo o robe del genere, ma sicuramente non ho detto niente di nuovo, perché chissà quanti lo hanno già chiesto. Scusate se il mio discorso è magari un po' vago e strampalato, ma spero che voi mi capiate...
saluti

L@Vipera

Mi pare che le risposte te le sei in parte date da solo. Su certi argomenti non possiamo essere completamente espliciti. E a ben vedere nemmeno lo vogliamo: per imparare davvero qualcosa non basta semplicemente leggerlo. Deve entrarti dentro perché hai provato e riprovato finché non hai compreso ogni passaggio. Noi ti diamo le basi, ti suggeriamo gli strumenti da usare, ti elenchiamo i link con i migliori siti sull'argomento. Il resto, purtroppo e per fortuna, devi mettercelo tu. Buon lavoro!

☺ Tech Humor ☺



"Il tasto che manca davvero sulle tastiere Windows."

☺ Tech Humor ☺



DEFINIZIONE DEL CARRO

Sono un newbie di 19 anni, vi ho scritto innanzi tutto per farvi i complimenti per la rivista (anche se, a volte, qualche articolo lascia a desiderare...) ma soprattutto perché siete stati i primi in Italia ad avere un'iniziativa del genere e perché cercate sempre di migliorare numero dopo numero. Studio all'università di Ferrara e tra i miei testi scolastici vi è un libro di "Fondamenti di informatica" (di cui tralascio i dettagli) in cui, secondo me vi è una definizione alquanto discutibile del termine Hacker, ve la trascrivo: "Hacker (parassita): pirata informatico che elude i sistemi di sicurezza, scoprendo password o sfruttando eventuali "buchi" nel sistema stesso, per entrare in banche dati o reti di computer. Questi tipi di azioni a volte sono puro divertimento altre volte vengono utilizzate per danneggiare istituzioni o apparati oppure per carpire dati (ad esempio lo spionaggio industriale)".
Ma secondo voi è giusto che un testo universitario debba dare un significato così approssimativo e diffamatorio degli hacker?!? Volevo chiedervi inoltre se potreste pubblicare questa lettera anche perché sto cercando di fondare un gruppo di appassionati alle prime armi di hacking e sicurezza, per formare un gruppo e organizzare ritrovi nella zona di Ferrara e dintorni. Se c'è qualche interessato può lasciare una mail a: nyoone@tin.it

.:NEO:. ($tefano83)

GUESTBOOK FRIENDS

Un saluto rapido ad alcuni amici che hanno lasciato messaggi simpatici nel guestbook di HJ: iustel, asprioV, VBInside, blobzapping, Hybrid, ^LorDFù§t^, Arj79, _-(-Kriég-)-_, Gelo33 (Angelo e Diana, felicitazioni), spaico man, lozio, JamesXr2i (in questo numero sei accontentato ;-), Zoelk, SkiFeZz.



HOT!

GIRO DI VITE SU DECODER E SOFTWARE

Piratare un decoder Stream o Tele+ può costare molto caro, ora: fino a tre anni di carcere e 15.000 euro di multa, con sanzioni anche per chi smercia e utilizza software non provvisto di licenza. Le pene più severe sono dirette a chi effettua copie per la vendita e alle aziende (che traggono dall'utilizzo del software un profitto commerciale). I privati, dal canto loro, sono perseguibili per ricettazione. Occhio quindi, che sono cambiate parecchio le carte in tavola, e giocare con le schede può essere molto rischioso.

DALLA CINA NO! AI WEBLOG

Dopo innumerevoli altri blocchi alla libertà di espressione in Rete, dalla Cina viene una ulteriore limitazione: l'impossibilità di accedere alla popolare comunità Blogspot.com, host di innumerevoli blog, lo strano miscuglio tra diario, rivista personale e album fotografico che è diventato ormai la mania online degli ultimi mesi. In questi giorni si celebra a Pechino un processo contro un attivista che avrebbe pubblicato notizie "disfattiste" sullo stato della Cina: la coincidenza sembra davvero eccessiva per essere davvero tale.

LIRVA ALL'ATTACCO DI AVRIL



Un nuovo virus, Lirva (w32.Lirva@mm), noto anche come Naith, si sta diffondendo attraverso Icq, Kazaa e mIRC. Colpisce solo chi non abbia installato la patch MS01-020 di Microsoft. Consiste in un messaggio che offre la possibilità di contattare la cantante pop Avril Lavigne, con oggetto, testo e allegati variabili. Cerca di rinviarsi a tutti gli indirizzi che trova nella rubrica di Windows e nei file con estensione dbx, .mbx, .wab, .html, .eml, .htm, .tbb, .shtml, .nch e .idx, cercando di chiudere gli antivirus e i firewall e di collegarsi il sito Web di Avril Lavigne.

NOVITÀ SUL DIRITTO D'AUTORE

Il Consiglio dei Ministri ha approvato una nuova normativa in materia di diritto d'autore, che riguarda soprattutto il sistema dei bollini e i relativi problemi correlati al software libero e alla sua distribuzione in Rete. Questa categoria di software è stato per l'appunto escluso dall'apposizione del bollino Siae, eliminando così le difficoltà che si incontravano in corso di distribuzione del software libero. In precedenza, l'apposizione del bollino o la stesura della dichiarazione sostitutiva era una procedura complessa e laboriosa, che limitava grandemente i canali di distribuzione libera, frustrando gli intenti di chi puntava sul software liberamente cedibile, modificabile e redistribuibile. Ora la burocrazia è stata semplificata, e le dichiarazioni possono essere cumulative per più versioni dello stesso software. Ugualmente, i supporti che contengono aggiornamenti, patch o altri software legati a programmi già usciti e volti esclusivamente al loro aggiornamento sono esenti dal bollino e dalle relative procedure, così come i sistemi operativi e il software preinstallato.

WINDOWS SI SPOGLIA

Bill Gates fa cadere il velo sul codice di Windows, mettendolo a disposizione di commissioni appositamente costituite per verificare la rispondenza a tutti i criteri di sicurezza informatica. In verità, andando a fondo nella notizia, si scopre che non è tutto oro quel che luccica. Saranno solo piccoli gruppi selezionati di tecnici a poter accedere al codice messo a disposizione da Microsoft, qualcosa di molto diverso dal pubblico dominio. Ma, considerando le abitudini alla riservatezza della casa di Redmond, questo rappresenta già un notevole passo in avanti. Il programma comprende per ora una decina di paesi e le corrispondenti commissioni nazionali, che potranno visitare il quartier generale di Microsoft, visionare la documentazione riservata sulla sicurezza, colloquiare con gli sviluppatori ed effettuare test, oltre a disporre — al 97%, il restante 3% è visionabile solo a Redmond - dei codici di Windows 2000, Windows XP, Windows CE e Windows Server 2003. Fra i paesi è compresa la Cina, che ultimamente aveva espresso pubblicamente le proprie preoccupazioni proprio in materia di sicurezza relativa all'utilizzo dei programmi Microsoft. Ma se la Cina lo aveva fatto apertamente, non è un segreto che il software Microsoft sia soggetto a bug corretti spesso solo in fase di aggiornamento, un mito che evidentemente Bill Gates cerca di sfatare.



INTEL CORRE A 64 BIT

Sono previste per questa estate un paio di interessanti novità: l'uscita di Madison, il successore di Itanium 2 McKinley, e di Deerfield, un Itanium 2 a basso consumo per sistemi a rack. McKinley avrà una cache da 6 Mbyte, il triplo di quella degli altri Itanium, con picchi di consumo attorno ai 130 watt, e conseguente necessità di un dispositivo di dissipazione più che adeguato (il radiatore di una vecchia Duna, per esempio). Ma è già in previsione un nuovo chip da ben 9 Mbyte di cache di terzo livello, atteso per il 2004, nonché, verso il 2005, Montecito, comprendente due unità di calcolo, quindi una vera e propria rivoluzione nel campo delle soluzioni dual processor, è già stata utilizzata per i chip Power4 di Ibm ed è prevista anche per i sistemi UltraSparc IV. Montecito sarà una novità anche per quel che riguarda la tecnologia, a 90 nanometri, un notevole progresso se confrontata con i 130 nanometri di Madison, Madison II e Deerfield e addirittura con i 180 nanometri di McKinley.

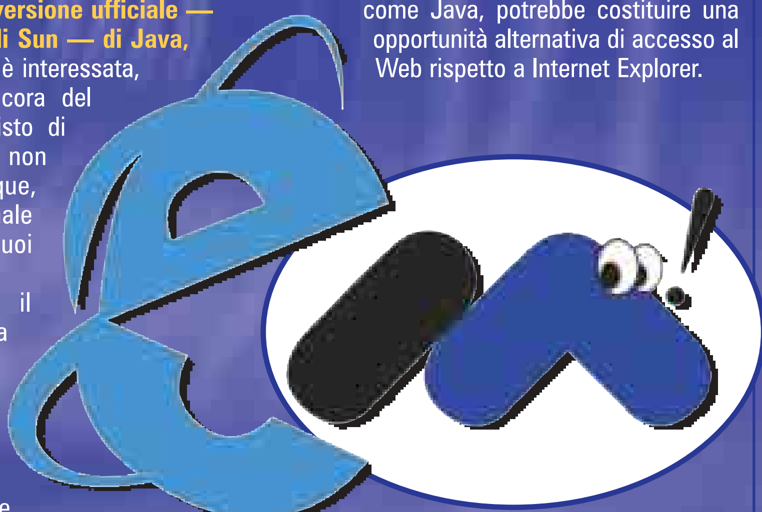
MICROSOFT, TORNA A JAVA

Dopo l'accusa a Microsoft, da parte dei legali di Sun, di aver sviluppato una versione del linguaggio Java proprietaria e incompatibile con quella "tradizionale", un giudice distrettuale americano J. Frederick Motz ha dato 4 mesi a Microsoft per reintrodurre il classico Java all'interno di Windows. Questo segue a una ingiunzione con cui Microsoft veniva obbligata ad inserire Java in ogni copia di Windows XP e nel Service Pack 2. Non riuscendo a giungere a un accordo sui tempi di realizzazione di tale iniziativa (la proposta di Sun era 90 giorni, quella di Microsoft 9 mesi), il giudice ha stabilito un limite di tempo intermedio. A questo punto, Microsoft ha due settimane di tempo per presentare un eventuale appello. E' facile comprendere le perplessità di Microsoft sull'apertura a Java: la versatilità e la interfacciabilità del linguaggio di programmazione succitato rischiano di minare seriamente il predominio dei prodotti Microsoft sul Web.



MICROSOFT VUOLE MACROMEDIA

Forse sull'onda dello smacco subito da parte di Sun, che per vie legali ha costretto Microsoft a integrare nei suoi sistemi imperativi la versione ufficiale — quella per l'appunto di Sun — di Java, la casa di Redmond si è interessata, secondo voci non ancora del tutto ufficiali, all'acquisto di Macromedia, che non naviga in buone acque, nonostante l'eccezionale successo dei suoi prodotti.
Perché collegare il contenzioso con Sun a questo ufficioso interessamento? Fra i prodotti di Macromedia, e forse quello che attualmente è più noto e utilizzato, c'è Flash, il noto software per la creazione di animazioni vettoriali, che è multipiattaforma (come Java), e che quindi, come Java, potrebbe costituire una opportunità alternativa di accesso al Web rispetto a Internet Explorer.



IL 3G NON DECOLLA

NTT DoCoMo Inc, maggiore operatore wireless giapponese (controlla circa il 60% del mercato nazionale) e attualmente unico operatore mondiale ad aver lanciato un servizio 3G sugli stessi standard previsti per gli operatori europei (lo standard WCDMA, Wideband Code Division Multiple Access), attraversa un periodo di crisi. I suoi servizi di terza generazione, lanciati un anno fa, dopo un boom iniziale dovuto forse più alla novità dell'offerta che a un reale riscontro nel campo delle esigenze dell'utente, sono fermi al palo. Il parco clienti previsto per il primo trimestre 2003 è stato ridotto previsionalmente del 77%. L'azienda attribuisce ufficialmente i problemi di gradimento a una bassa durata delle batterie dei cellulari (attualmente 100 ore in standby, mediamente il doppio di quelle dei tradizionali telefonini, ma secondo l'azienda ancora non sufficienti) e a una copertura dei servizi non totale (per ora l'82% del territorio). I nuovi terminali (prodotti da NEC, Fujitsu e Matsushita), avranno batterie di durata in standby vicina alle 180 ore.

HOT!

MEMORY STICK A 32 GB



Il settore dei supporti di memoria è quantomai vario e ivi la concorrenza è decisamente agguerrita: SmartMedia, CompactFlash, Secure Digital, MultiMediaCard. Sony, nel tentativo di rendere le Memory Stick il formato digitale universale per il trasporto e lo scambio di dati digitali, sta puntando su una nuova tecnologia, *Memory Stick Pro*, in grado di arrivare, in un prossimo futuro, alle incredibili dimensioni di 32 GByte. Per il momento, si cominceranno a trovare sul mercato carte da 256 Mb, 512 Mb e 1 Gbyte, al prezzo previsto di, rispettivamente, 190, 440 e 880 dollari.
Su dispositivi appositamente concepiti, è assicurato un alto livello di sicurezza: l'accesso ai dati può essere bloccato.
Anche l'attuale disponibilità di Memory Stick è stata aggiornata: la capacità è stata portata a 256 Mbyte, seppure si tratti di una tecnologia più lenta, meno adatta all'utilizzo in palmari e dispositivi portatili in genere.

REFERENDUM SUGLI HACKER



Negli Stati Uniti la Commissione incaricata di stabilire le regole per le sentenze federali ha chiesto consiglio alla pubblica opinione per trovare una formula adeguata in materia di cracking e virus writing. In pratica, si chiede consiglio sulla formula da utilizzarsi nei processi, per rendersi conto di quale sia il parere del cittadino, e se le pene attuali siano commisurate al reato. La direzione in cui vorrebbe andare il governo statunitense è quello di una recrudescenza delle pene, proponendo una sorta di "metodo a punteggio", per cui le aggravanti e le attenuanti varierebbero la pena finale. Attualmente i reati informatici sono inseriti nella fascia dei reati di furto o danneggiamento, ma secondo la Commissione ciò non è realistico, in una società sempre più dipendente dall'informatica.

HOT!

3, PRONTI, VIA

Dopo una sofferta e continuamente dilatata fase preliminare, l'operatore di telefonia mobile di terza generazione 3 pone una nuova data di esordio ufficiale: il 1 febbraio 2003 (perché il primo e non il "3"?). Secondo i vertici di 3, i primi clienti (circa 300 privilegiati) riceveranno il loro cellulare Umts entro la fine di gennaio; altri 110.000 terminali saranno consegnati da febbraio in poi ai clienti con opzione Top Privilege. Il telefono scelto dall'azienda è il NEC e606, già protagonista del roadshow natalizio nei negozi affiliati.

GPRS FLAT CON TIM

Tim ha lanciato, dopo una fase promozionale, il servizio "GPRS Free Internet", che permette di navigare senza limiti di tempo o traffico per 30 giorni con il GPRS Web al costo di 20 euro (il traffico WAP è escluso). L'offerta è compresa nell'acquisto di un nuovo cellulare Tim GPRS dal 13 gennaio al 6 aprile.

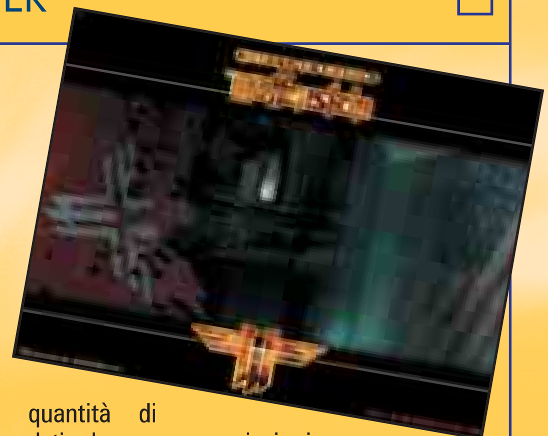
CONTRATTI ONLINE SICURI

Da Deedgital sta per arrivare un software per stipulare contratti elettronici in completa sicurezza. Il programma registra su un file video, certificato da chiave digitale, tutti i passi percorsi dall'utente per suggellare un contratto in Rete, permettendo poi di produrli in caso di controversie.

ASSOLUZIONE PER DECSS

Brutto colpo per i paladini del copyright: l'autore di DeCss, un programma in grado di oltrepassare la protezione crittografica dei DVD per poterli utilizzare liberamente su qualsiasi sistema, in un primo tempo condannato, è stato ora assolto.La sentenza precisa che non si può individuare un reato nel procurare l'accesso in qualsiasi condizione a dati che sono regolarmente in nostro possesso. Inoltre, la possibilità di duplicazione è presente solo come "effetto secondario": lo scopo primario è quello della fruizione dei dati.

DDOS DAI GAME SERVER



DivX Solutions, azienda che opera nel campo della sicurezza, ha individuato una vulnerabilità nei server del network di multiplaying GameSpy, che potrebbero essere utilizzati da un aggressore per amplificare l'effetto di un attacco DDoS.

I game server di questo circuito, in molto casi, rispondono automaticamente alle interrogazioni sullo stato del servizio senza controllare l'IP del mittente. Se un cracker inviasse a uno di questi server molteplici richieste aventi come mittente l'IP del sistema da attaccare, ben presto il sistema si saturerebbe.

I server vulnerabili sono molti, e comprendono piattaforme per giochi come "Quake 2" "Half life", "Neverwinter Nights" e "Return to Castle Wolfenstein". L'azienda si è già mobilitata per evitare questo inconveniente, promettendo per tutti i server del sistema una patch che limiti la quantità di dati che un server invia in risposta a una interrogazione. Se questo non risolverà completamente il problema, permetterà comunque di poter usufruire dei servizi online avendo a disposizione la banda passante necessaria e evitando per quanto possibile l'utilizzo dei server come basi di attacco DDoS.

PALM SI LASCIA ALLE SPALLE GRAFFITI

Graffiti, il celebre e apprezzato sistema di riconoscimento della scrittura naturale di Palm, sarà presto sostituito da una versione rielaborata di Jot, un software già oggi utilizzato come metodo alternativo a Graffiti su molti palmari, e che verrà chiamata Graffiti 2.

La spinta primaria che ha portato a tale decisione è stata di natura legale: Palm è coinvolta da quasi sei anni in un interminabile procedimento legale, che a tutt'oggi vede una situazione di stallo, che la vede contrapposta a Xerox per la paternità della tecnologia su cui si basa Graffiti, ovvero la possibilità di scrivere tutti i caratteri con un unico segno ininterrotto. Ma anche la funzionalità vuole la sua parte: il nuovo software permette di scrivere in ogni parte dello schermo e in modo più naturale. Si potrà anche "addestrare" il sistema a riconoscere la propria particolare scrittura.

Ad ogni modo, le ricerche di mercato individuano una tendenza al ritorno alla tastiera, soprattutto se si verificano le statistiche di vendita dei palmari Handspring che di tastiera, appunto, sono dotati.

RADEON E DIVX INSIEME

ATI ha deciso di supportare DivX, studiando con i suoi programmatori una versione ottimizzata del codec per sfruttare al meglio i più recenti chip grafici Radon, il 9500 e il 9700. La nuova tecnologia sfrutterà i pixel shaker attraverso la tecnologia FullStream, riducendo quindi la scarsa niditezza dello streaming video tipica di DivX. Oltre a questo, l'utilizzo della CPU viene diminuito, e le prestazioni video aumentate fino al 50% (in post processing).

C'è da dire che non si tratta del primo accordo commerciale: molte altre intese sono state segnate con produttori di console, player multimediali e software, per l'implementazione del popolare algoritmo nei propri prodotti.

DivX gode di grande popolarità, ormai, fra i codec compatibili con MPEG-4, nonostante debba vedersela con giganti del calibro di Real Networks e Microsoft Windows Media, costantemente aggiornato e con prestazioni continuamente incrementate.

HOT!

MORPHEUS RIPRENDE VITA

StreamCast Networks, distributore del client peer to peer, sta per immettere in circolazione una nuova versione del software, nel tentativo di riconquistare i favori del pubblico dopo i recenti problemi, soprattutto di natura legale (che, si dice, rischiano di far chiudere l'azienda in pochi mesi, in mancanza di una soluzione favorevole). E questo "colpo di testa" non favorirà certo la posizione dell'azienda, data l'estrema versatilità del motore di ricerca e delle nuove funzionalità.
La nuova versione di Morpheus potrà essere gestita automaticamente, programmando ricerche e partendo subito con lo scaricamento una volta reperiti i file cercati. La ricerca potrà estendersi, in caso di esito negativo, ad altri sottonetwork, facilitando il reperimento di pezzi anche molto rari.



CONSOLE PER MAME



Un californiano sta progettando una console su misura per le Rom di MAME, il celebre emulatore italiano di vecchi coin-op da bar e console di gioco ormai estinte. Questo dispositivo, oltre a dare un diverso feeling al gioco (la console non sarebbe molto dissimile da una Playstation o un Xbox) porterebbe a una regolarizzazione del mercato delle Rom, da sempre al centro di polemiche e discordi valutazioni legali. Sarebbe inoltre un modo per avvicinare al mercato delle console tutti i nostalgici giocatori di qualche anno fa, poco attratti dai moderni sparatutto 3D e desiderosi solo di riprovare le emozioni delle amate macchinette da bar. La console MAME potrà essere connessa a una TV o a un monitor VGA, e disporrà di una porta USB per la connessione di tastiere, game pad e joystick. Avrà un lettore DVD-ROM e, forse, un hard disk.



Non ci sono ancora ipotesi fondate sulla configurazione, ma si pensa che, per ridurre i costi e ottimizzare le prestazioni, ci si baserà su ordinari componenti per Pc e su Linux. Il prezzo potrebbe aggirarsi sui 200/300 dollari, e comprenderebbe una dotazione di Rom di giochi.



SQL SERVER 2000, TERZO SERVICE PACK

È da pochi giorni disponibile sul sito Microsoft il Service Pack 3 (SP3) per il database SQL Server 2000. Esso consiste di due file: il primo, di circa 45 MB, con le versioni aggiornate dei componenti del database; il secondo, di circa 57 MB, con le versioni aggiornate dei componenti dei servizi di analisi.
SP3 contiene tutte le patch rilasciate dalla prima edizione di SQL Server 2000; fra le migliorie apportate, il report degli errori e l'amministrazione multiserver.

GALERA PER UNA FRASE SUL WEB?

Un cittadino tedesco, dopo aver inserito frasi decisamente discutibili sull'attentato dell'11 settembre alle Twin Towers (complimenti agli attentatori e accuse agli Stati Uniti), seppur precedute da un disclaimer in cui l'autore si proclamava un antimilitarista convinto in vena di provocazioni, è stato segnalato alla magistratura. L'uomo è stato chiamato in aula per rispondere dell'accusa di aver inneggiato a un crimine e aver oltraggiato la memoria delle vittime. La storia è comunque a lieto fine: il giudice ha assolto l'uomo dopo averlo ritenuto non realmente favorevole al crimine. Secondo il magistrato, senza quel disclaimer l'autore avrebbe meritato la galera, ma il richiamo era indispensabile perché il rischio che qualcuno leggesse la frase senza vedere prima il disclaimer era alto. Questo nonostante la legge tedesca punisca pesantemente anche la semplice apologia: ma le grida contro il tentativo di violazione della libertà di espressione si sono, naturalmente, levate alte.

PROTEGGERE SENZA BLOCCARE

Microsoft ha allo studio una nuova tecnologia di protezione dei CD, che, a differenza delle altre, permetterà di riprodurli su qualsiasi supporto, a differenza di quel che accade oggigiorno. La tecnologia, denominata Windows Media Data Session Toolkit (WMDST), si limiterà a impedire la copia del CD, ma non ne inibirà l'usufrutto in alcun modo. Per rendere possibile questo, il supporto conterrà sia le tradizionale tracce musicale che una versione codificata in Windows Media Audio e riproducibili su di un PC.

VULNERABILITÀ DHCP

Il software ISC DHCPS, nella versione 3 (e fino alla 3.0.1RC10) è soggetto a gravi bug di buffer overflow, che potrebbero essere sfruttati inviando messaggi DHCP con nomi di host lunghi, utilizzando la funzionalità di aggiornamento automatico di un server DHCP. Il cracker potrebbe accedere al server ed eseguire comandi con gli stessi privilegi dell'amministratore. L'upgrade a una release successiva risolve ogni problema.

NEWBIE

UN PO' D'ORDINE SUL DISCO



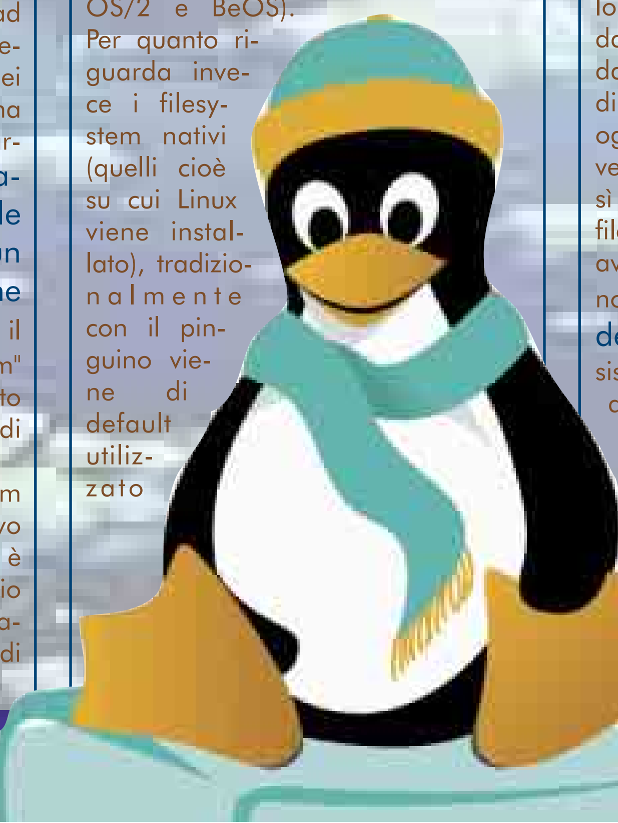
Prima ancora di installare Linux, bisogna porsi il problema del tipo di struttura che i dati dovranno avere sul disco. Ecco una guida ragionata alle varie opzioni disponibili.

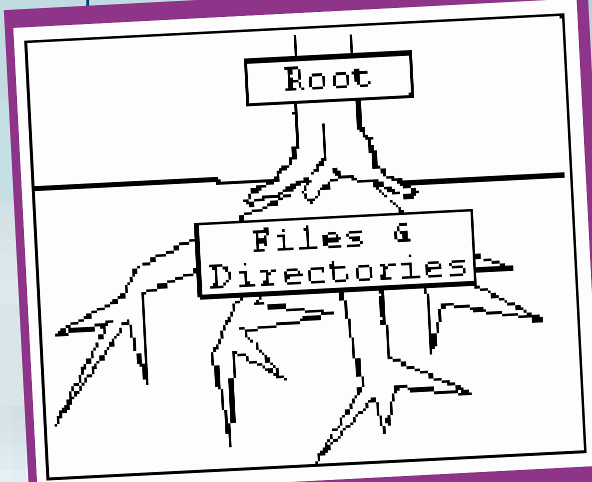
CONOSCERE E CAPIRE I FILESYSTEM DEL PINGUINO

Son il termine filesystem si indica il metodo e le strutture di dati che un sistema operativo utilizza per gestire i file presenti su un unità fisica (floppy, hard disk, CD-Rom...) o su una sua partizione: compito del filesystem (abbreviato spesso in fs) è quindi quello di fornire meccanismi per identificare il file ed accedere ad essi, gestire lo spazio libero ed implementare meccanismi di protezione dei dati memorizzati sul supporto. Prima di poter utilizzare un disco o una partizione come filesystem, è necessario inizializzarlo in maniera tale da predisporlo ad utilizzare un determinato sistema di gestione dei file; questa operazione prende il nome di "creazione di un filesystem" (ed è un po' quello che fa il tanto amato/temuto comando format di DOS).

Le caratteristiche dei diversi filesystem variano in base al sistema operativo utilizzato, e anche GNU/Linux non è da meno, visto che utilizza un proprio filesystem in maniera nativa ma tuttavia ne supporta altri esistenti, tipici di diversi sistemi operativi (per esempio per lo scambio di file, ma non solo..). Tra i file system supportati troviamo ovviamente ISO9660 (il fs standard per i CD-Rom), mdos, vfat (Windows 9x/Me), NTFS (il fs di Windows NT, supportato però in sola lettura), hpfs e befs (cioè i fs nativi rispettivamente dei gloriosi OS/2 e BeOS).

Per quanto riguarda invece i filesystem nativi (quelli cioè su cui Linux viene installato), tradizionalmente con il pinguino viene di default utilizzato l'ext2 (filesystem esteso di tipo 2), introdotto già nel 1995 con il kernel 1.2. Ext2 in effetti si è dimostrato negli anni un filesystem efficiente, affidabile e decisamente veloce; tuttavia in caso di sbalzi di corrente o di riavvii indesiderati, un possibile perdita dei dati è sempre in agguato. Infatti un filesystem non si occupa solo di gestire i singoli file bensì anche i dati relativi ad essi, i cosiddetti metadata (allocazione fisica sul dispositivo, dimensione...). È evidente come, a ogni modifica, il sistema debba provvedere ad aggiornare i metadata, così da mantenerli sempre allineati con i file presenti. Se il blocco del sistema avviene prima che i metadata vengano sincronizzati, si hanno quindi dei disallineamenti; compito del sistema operativo sarà quindi quello di provvedere immediatamente a verificare l'integrità dell'intero fs allo scopo di individuarli e correggerli. Tutto ciò si traduce nell'esecuzione (al momento del primo riavvio) del programma fsck; questa sorta di "Scandisk per il pinguino",





Lo schema delle directory standard dei sistemi Unix.

oltre a bloccare anche per lungo tempo il sistema, non sempre riesce nell'intento di recuperare i file disallineati.

>> Un diario di bordo...

In questi ultimissimi anni sono quindi nati dei nuovi filesystem in grado di mantenere integri i dati anche in caso di crash o di spegnimento anomalo. Questi file system, detti journaled fs, mantengono un file di log (o journal, diario) in cui viene registrata ogni operazione compiuta sui file stessi; pertanto, se anche questi ultimi non venissero applicati fisicamente, il journaled filesystem riuscirà comunque al successivo riavvio, basandosi sul file di journal, a recuperare tutti i dati e le modifiche non salvate, riportando il sistema nella condizione precedente il blocco. Questo ovviamente rende il reboot molto più rapido, e garantisce un elevata sicurezza dei dati. Non occorre però dimenticare che il file stesso di journal occupa spazio, e richiede un continuo aggiornamento, cosa che "ruba" risorse preziose al sistema. I principali fs di questo tipo disponibili per Linux sono essenzialmente quattro:

• ReiserFS Inserito ufficialmente nel kernel stabile sin dalla release 2.4.1, questo fs è per molti aspetti decisamente innovativo ed è "sponsorizzato" da nomi decisamente di spicco (SuSE Linux in primis).

• Ext3 Come dice il nome stesso, Ext3 è in pratica un Ext2 con in più il supporto per il journaling. Sviluppato principalmente da Red Hat, semplifica notevolmente la conversione da partizioni Ext2.

• XFS e JFS Questi due filesystem, un tempo disponibili solo per gli Unix proprietari rispettivamente di SGI (Irix) e IBM (AIX), sono stati recentemente portati dalle stesse aziende su piattaforma Linux e rilasciati sotto licenza GPL; al momento sono ancora abbastanza instabili e, non essendo inclusi nel kernel (al contrario degli altri due sopra citati), possono essere installati come patch.

I COMANDI per il file system

Molti di voi troveranno comodo aggirarsi per il filesystem utilizzando l'interfaccia grafica; i più coraggiosi di voi però avranno già aperto un terminale e messo il mouse sotto naftalina... Per questi ultimi presentiamo un lista dei comandi di base da utilizzare sotto Linux per giocherellare con i file e le directory

- **man** ➜ mostra la pagina del manuale di un determinato comando (RTFM!!)
- **ls** ➜ lista il contenuto di una directory
- **cd** ➜ per cambiare direcotry
- **pwd** ➜ visualizza il path della directory corrente
- **file** ➜ indica il tipo di file
- **cp** ➜ per copiare file
- **mv** ➜ per spostare o rinominare file
- **rm** ➜ per rimuovere file
- **mkdir** ➜ per creare directory
- **rmdir** ➜ per eliminare directory
- **cat** ➜ visualizza il contenuto di un file
- **df** ➜ mostra lo spazio disponibile sui dischi
- **du** ➜ mostra lo spazio occupato da file e/o directory
- **clear** ➜ pulisce lo schermo del terminale

Ricordatevi che Linux è case sensitive (ovvero vi è differenza tra lettere maiuscole e minuscole), che i file che iniziano con un punto sono considerati come file nascosti e che quelli che terminano con la tilde (~) sono file di backup. Inoltre, evitate di lavorare normalmente come root (un sistema non danneggiato è buono per un'altra volta! :) e, soprattutto, se non sapete cosa state facendo, non fatelo! (vedi sopra... :).

>> A spasso tra file e directory

La struttura delle directory di Linux è simile a quella che si riscontra in altri Unix o sotto DOS, ed è organizzata in modo gerarchico (è perciò un HFS, Hierarchical File System), strutturata

secondo uno schema tipo albero. Al livello più elevato c'è la directory principale, indicata come directory root di sistema (dall'inglese root, radice appunto); questa, indicata con '/', è l'unica directory presente a questo livello e tutte le altre sono referenziate nel loro path, o percorso, in rapporto ad essa (per esempio /etc è un sottodirectory di primo livello di /). Come avrete già notato, al contrario di DOS/Windows, in Linux (ma più in generale sotto Unix) viene utilizzata la barra (/) per indicare i path delle directory. Altro elemento di primaria importanza da considerare è il fatto che sotto questi OS il sistema faccia riferimento a un unico grande albero delle directory. Questo significa che le diverse partizioni e i vari dispositivi non saranno accessibili tramite lettere di unità, bensì verranno "montate" in sottodirectory di root; per approfondire l'argomento date un occhiata al riquadro presente in queste pagine dedicato proprio al concetto di mounting.



Già al primo avvio si può notare, con un certo stupore, la presenza di un gran numero di directory dai nomi apparentemente misteriosi (/mnt, /etc, /usr...). Tutto questo è però forse più comprensibile se si premette che in Linux i file vengono memorizzati in diverse posizioni del filesystem in base alla loro funzione e tipologia e non tanto divisi per singole applicazioni (come solitamente accade i Windows). Ecco che troveremo quindi una directory contenente quanto necessario per l'avvio del sistema, una per i file temporanei, una per i log e una per i file di configurazione, una contenente i tool per l'amministrazione di base del sistema, una per le directory personali degli utenti e così via... Inoltre alcune direcory, come /de e /proc, contengono file molto particolari che meritano un discorso a parte; non temete: torneremo in seguito sull'argomento.

Ben presto, con il nascere delle prime distribuzioni, si avvertì l'esigenza di creare uno standard per la disposizione di file e directory in Linux; nacque quindi nel 1993 il progetto Filesystem Standard (o FSSTND), poi ribattezzato Filesystem Hierarchy Standard (liberamente consultabile all'indirizzo http://www.pathname.com/fhs/). L'attuale organizzazione dei file in una distribuzione dovrebbe tener conto di quanto stabilito da questi standard, che peraltro permettono agli sviluppatori di creare software senza doversi preoccupare di problemi di compatibilità tra le diverse distribuzioni.

lele - www.altos.tk

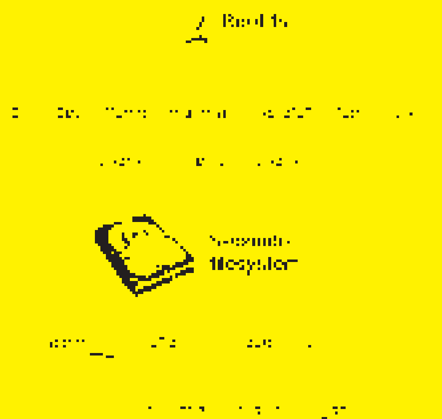




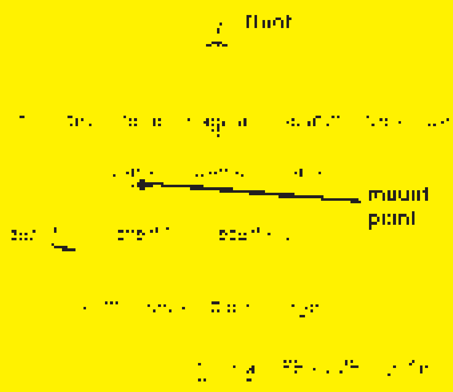
ScanDisk di Windows;
fsck è l' equivalente Unix.

Perchè un filesystem sia accessibile da Linux, occorre prima effetturare il mount. I filesystem possono essere raggruppati in maniera logica da sembrare uno solo; le partizioni rimangono separate ma appaiono come appartenenti ad un singolo albero delle directory. I dispositivi esterni (floppy, CD-Rom...) vengono montati all'interno della directory /mnt appositamente creata (/mnt/floppy, /mnt/cdrom...), anche se nulla vieta di montarli in un altro punto dell'albero. Per visualizzare un elenco dei filesystem montati è sufficiente eseguire il comando mount senza parametri. Per effettuare il montaggio di un particolare dispositivo bisogna usare sempre il comando mount con due argomenti: il dispositivo fisico da montare e il punto di montaggio.

I filesystem prima del mount



Situazione dopo il mount



UNO DEI PIÙ DIFFUSI SOFTWARE PER SCAMBIARE FILE, MUSICA E VIDEO

KAZAA
la parola magica

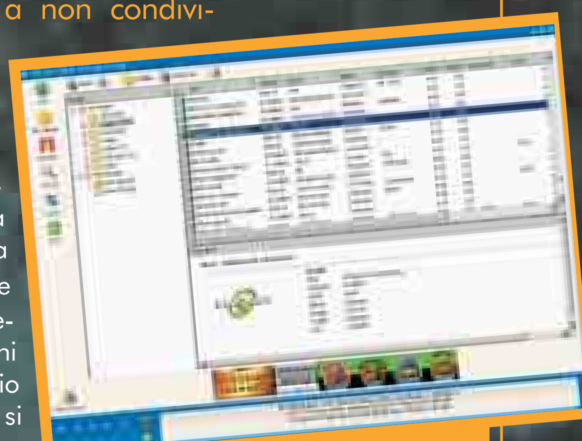


Kazaa, figlio di Morpheus, edere di Napster: sembra la genealogia di una famiglia del Signore degli Anelli, invece è un interessante sistema di file sharing.

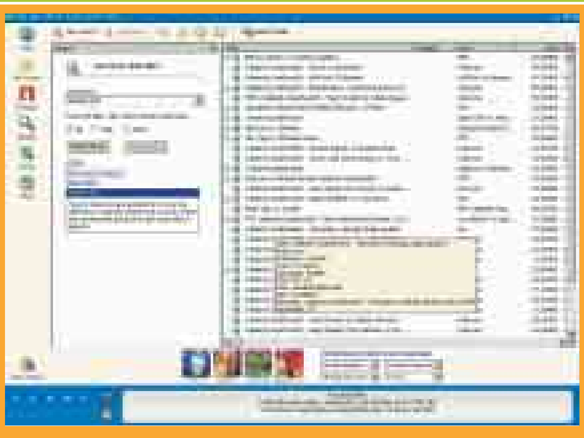
Il concetto di file sharing è ormai noto a tutti: consiste nella condivisione di file con altri utenti attraverso software dedicati. Parliamo proprio di uno di questi software, Kazaa, giunto alla versione 2.0 dopo diverse traversie. Kazaa è infatti "figlio" di Morpheus, uno dei più celebri eredi del dopo Napster, che godette di grande successo finché conflitti di gestione aziendale non portarono al distacco della "costola Kazaa". Il motore è lo stesso, del tutto simile l'interfaccia, molto diversi i successi: Morpheus è rimasto nella polvere, mentre Kazaa è assurto agli altari del file sharing.
Scarichiamo l'installer dal sito ufficiale, www.kazaa.com. Come per la maggior parte dei programmi moderni, si tratta di un file di dimensioni minime, che poi si collegherà, nuovamente al sito, per scaricare i componenti necessari. È giusto ricordare subito che Kazaa si basa, nel vero senso della parola, sullo spyware. In esso è incorporato un componente, Cydoor, che raccoglie informazioni sui gusti degli utenti per proporre poi spot appropriati. Inutile dire che la rimozione di Cydoor bloccherà anche l'utilizzo di Kazaa. C'è in circolazione, in verità, anche una versione rigorosamente non ufficiale, detta Kazaa Lite e che funziona senza banner, ma non è aggiornata, e non possiamo davvero essere sicuri che non vi si annidi qualcosa di peggio. In fase di installazione ci viene richiesta la destinazione dei file scaricati e le cartelle che vogliamo condividere (facciamo attenzione a non condividere tutto il disco).



Dovranno essere inseriti uno username (che ci identificherà sul sistema nella forma user@kazaa) e una e-mail (per ricevere i soliti bollettini informativi). All'avvio del programma, si possono impostare queste ed altre opzioni: possiamo scegliere se lanciare o no Ka-



La finestra dalla quale si può ispezionare la propria collezione di file condivisi.



Da qui si possono cercare e scaricare i file presenti sui computer degli altri membri della comunità.

zaa all'avvio di Windows, porre limiti al numero di upload o di download contemporanei, sospendere la condivisione di file (solo in casi eccezionali, mi raccomando) o abilitare la scansione antivirus dei file condivisi, limitare il numero dei risultati di una ricerca, filtrare i file scaricabili da bogus (file fasulli) o contenuti non opportuni, gestire il firewall, lo scambio di messaggi con altri utenti e le skin.



>> Utilizzare Kazaa

La barra degli strumenti in alto varia a seconda delle schermate selezionate a sinistra, e riporta i comandi principali operativi in quella sezione. La schermata principale, Web, è un browser vero e proprio, e presenta il messagio di benvenuto, con news e pubblicità varie.

My Kazaa permette di visualizzare quali file stiamo condividendo, editandone i dettagli, che saranno utilizzati come parole chiave e visualizzati in fase di ricerca e di download sul network, aggiungendoli alle nostre playlist e con una valutazione sulla qualità del file (da Poor a Excellent), così chi sceglie di scaricare un file da noi ne vede lo stato.

Theater è una sorta di player, che può essere utilizzato per vedere e ascoltare file multimediali e che consente, in caso di Mp3 e filmati Mpeg, di avere un'anteprima del file che stiamo scaricando, in modo da verificare che sia proprio quello che vogliamo (alzi la mano chi non ha mai scaricato da Kazaa cose che non avevano nulla a che fare col titolo...).

Search è la finestra di ricerca per chiave.

Si può effettuare una ricerca generica, o limitarla ai file audio, video, alle immagini, ai documenti, al software o alle playlist. Possiamo anche decidere di effettuare la stessa ricerca sul Web. I risultati che compariranno nella finestra a destra sono estremamente dettagliati, e contengono le dimensioni, il tempo stimato di scaricamento (approssimativo), la banda sfruttabile, il tipo di file, la sua categoria (genere musicale o cinematografico) e lo username dell'utente che lo sta condividendo (o diciture come "2 users" se è messo a disposizione da più persone). Visto che Kazaa supporta lo scaricamento a segmenti (e ogni scaricamento è recuperabile in un secondo tempo), più utenti hanno lo stesso file, più agevole sarà il download. Ponendo il mouse sopra il file, una finestra di popup ci riporta altri particolari. Basta fare doppio click sul file per scaricarlo.



L'unico sistema che premia i più generosi

Il livello di partecipazione è una novità dell'ultima edizione di Kazaa: si tratta di un numero, da 0 a 1000, e un simpatico titolo (il massimo è Supreme Being (essere supremo), passando per Deity (semidio) e via dicendo. Tale valutazione viene attribuita a un utente secondo la quantità e qualità dei file che mette a disposizione, dando all'utente stesso privilegi nelle liste d'attesa.

È possibile taroccare il proprio livello di partecipazione col Registro di Windows o con appositi programmini. Ma, siccome l'idea di favorire chi partecipa più attivamente alla comunità ci piace, non vi diremo come fare :-D



>> Controlli avanzati

Traffic è dove visualizziamo il traffico in entrata e in uscita. Nella finestra superiore le nostre selezioni, in quella inferiore i file scelti dagli altri utenti fra quelli che condividiamo. I dettagli sono molteplici e facendo clic destro sui file, possiamo scegliere di bloccare o sospendere il download o cercare altre fonti da cui scaricare nonché effettuare sottoricerche sullo stesso autore e scrivere un messaggio all'utente. Shopping è nulla più che una vetrina venduta agli sponsor.

Un'ultima raccomandazione: non basta il clic sulla X in alto a destra per chiudere Kazaa. Dovremo fare un clic destro sulla sua icona nella barra e scegliere di chiuderlo per farlo sparire del tutto.

Paola Tigrino

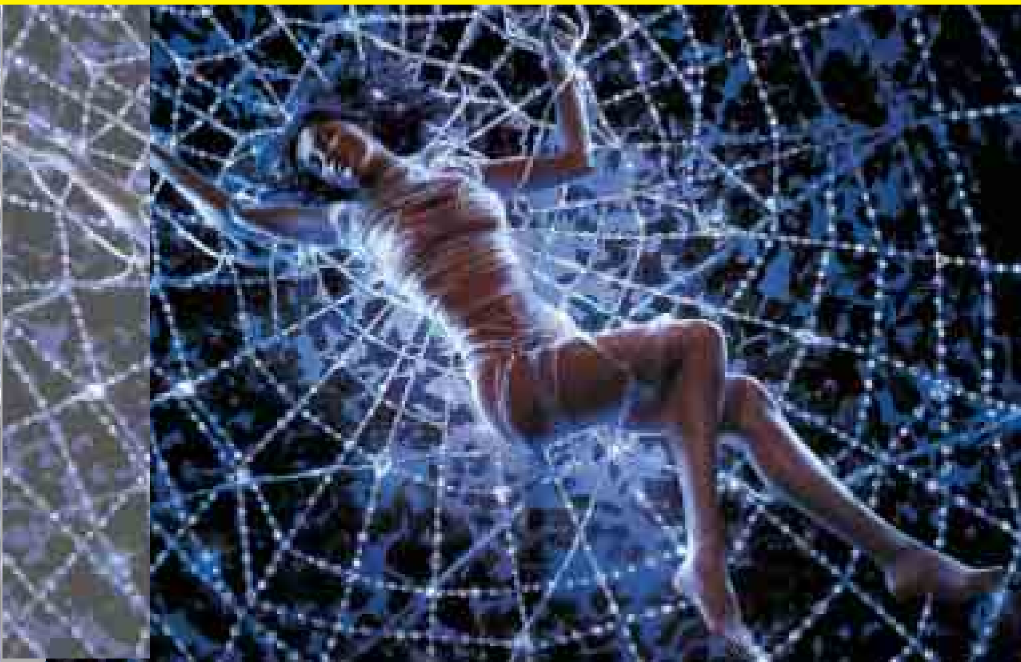


Dal pannello *Traffic* controlliamo i trasferimenti, e scarichiamo uno stesso file in parallelo da più utenti.

LE PRINCIPALI FALLE DEI SERVER WEB

I buchi nella ragnatela

La maggior parte dei server accessibili al pubblico sono server Web; facile immaginare che proprio questi siano il bersaglio più comune di cracker e lamer di ogni sorta.

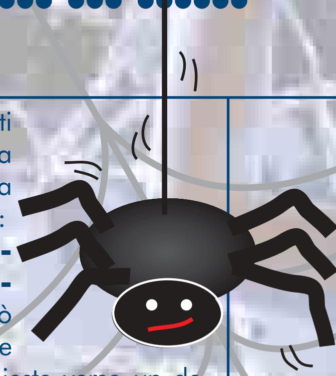


Tutti i server che gestiscono Internet, di qualunque natura essi siano, sono definibili come dei daemon (demoni). Un daemon altro non è se non un programma che lavora in background svolgendo svariate funzioni e attivandosi al momento più opportuno, senza bisogno di nessuna azione da parte dell'amministratore. I servizi Web, FTP, Mail, Telnet e svariati altri ancora sono tutti daemon che si attivano al momento dell'avvio del computer, e rimangono in attesa di una richiesta, ricevuta la quale attiveranno il servizio associato. Un daemon FTP, per esempio, è un programma che sta in ascolto, normalmente sulla porta 23 e che nel momento in cui giunge una richiesta di comunicazione si attiva restituendo l'output più opportuno per quella situazione specifica.
Di certo i server Web sono fra i daemon più utilizzati e performanti, ma al tempo stesso, proprio a causa di questa loro larga diffusione, sono anche i più studiati e attaccati dai cracker che sfruttano a modo loro i bug inevitabilmente presenti nei codici.
Apache, IIS, Lotus e Novell sono solo alcuni dei server Web più utilizzati; il nostro compito sarà quello di cercare di analizzare queste applicazioni e vedere i loro punti deboli, con uno sguardo sempre rivolto alla sicurezza ed alla risoluzione dei problemi.

>> Apache server http



È sviluppato da una collettività di utenti (www.apache.org), ed è stato fin dall'inizio degli anni '90 il server Web più diffuso (prima del '95, Apache si chiamava "NCSA httpd"). E' un software distribuito gratuitamente assieme a molte distribuzioni Unix, e proprio in virtù di ciò il suo codice è pubblico e migliorabile da chiunque.



I rischi documentati per ciò che riguarda questa piattaforma sono essenzialmente:

1. **Attacco Denial of Service:** un cracker può mandare una serie innumerevole di richieste verso un determinato dominio Web aggiungendo all'indirizzo un numero molto grande di caratteri "/". Il sistema non reagisce e si viene a creare una congestione della CPU, con il conseguente blocco del servizio. Le versioni "attaccabili" con questo metodo solo la 1.2.5 e le precedenti.

> **?** **DoS** (Denial of Service): un attacco che mira a rendere inagibile un server o un servizio, per esempio sovraccaricandolo o provocando errori e blocchi di sistema.

2. **Attacco CGI:** più che un attacco si tratta di un furto, dato che la versione 1.3.12 di Apache permette di "rubare" gli script CGI accedendo direttamente alla cartella /cgi-bin/.
3. **Visualizzazione delle directory e del loro contenuto:** le versioni Apache 1.3.3, 1.3.6, 1.3.12 permettono la visualizzazione delle directory e del loro contenuto. La situazione si sviluppa quando un percorso è molto lungo ed il server va alla ricerca del file di avvio (avvio.html). Come risultato di questo processo si ha la visualizzazione della directory, che sia presente il file di avvio o meno.
4. **Esecuzione di codici:** in una nota rilasciata nella metà di giugno si afferma che esiste un bug pericolosissimo che affligge le versioni

comprese fra la 1.3 e la 1.3.24 attraverso il quale un hacker può eseguire un codice arbitrario da remoto sulla macchina server. E' stato considerato un bug talmente importante da meritare un avviso diretto di Apache con richiesta di caricare la patch entro due giorni.

>> Microsoft Internet Information Server



È sviluppato da Microsoft ed è il concorrente naturale di Apache. Si integra perfettamente con Windows NT e funziona anche da server intranet. È molto funzionale per l'utenza, in quanto configurazione può essere fatta tutta in modo grafico, e risulta quindi alla portata anche di Webmaster meno esperti. Proprio per questo però, è molto probabile trovare in giro server IIS configurati male, per inesperienza del Webmaster.
I rischi documentati per questo tipo di pacchetto sono i seguenti:

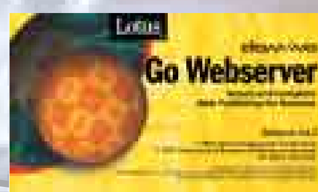
1 **Attacco Denial-of-Service:** le versioni IIS 3 e 4 sono sensibili a un attacco DoS che porta all'interruzione del servizio tramite l'invio di richieste GET. Questo tipo di richieste altro non sono che l'equivalente della cattura dei files in riga di comando. Se vengono lanciate numerose richieste GET sbagliate si consumano risorse tanto da arrivare al blocco totale del servizio.

2 **Attacco Sioux Denial-of-Service:** anche questo colpisce le versioni IIS 3 e 4 e provoca la repentina congestione della CPU. Si effettua tramite l'utilizzo di un programma chiamato Siuox.c facilmente reperibile in rete. La sua esecuzione contro indirizzi Web sensibili fa salire immediatamente l'utilizzo della CPU oltre i valori di 90%.

3 **Attacco con Cavallo di Troia:** nella versione IIS 4 è possibile eseguire un codice su un daemon che funziona come un cavallo di Troia garantendo un accesso non autorizzato e la possibilità di eseguire codici remoti. L'attacco si basa su un buffer overflow legato al codice htr/ism.dll che permette di sfruttare questo attacco. Lo script HTR è utilizzato in IIS per cambiare le password via Web; per funzionare questo servizio utilizza la ism.dll che però, se opportunamente sfruttata, può creare un buffer overflow di sistema.

4 **Attacco codice ASP:** le versioni vulnerabili sono la IIS 3 e 4 e la vulnerabilità consiste nella sottrazione del codice. Normalmente gli stream generati da IIS sono salvati sottoforma di nomefile:stream e quindi possono essere richiamati con un indirizzo del tipo www.bersaglio.com/file.asp::$DATA ottenendo così il codice generante e non l'output.

>> Lotus Domino



Quella di Domino (www.domino.lotus.com) è un sistema Web soprattutto orientato alle aziende che permette applicazioni Web e scambio di messaggi.
Ecco i rischi documentati:

1 **Attacco per sottrazione di codice:** tutte le piattaforme Domino sono sensibili a un attacco destinato a rubare codice sorgente. Il baco permette di navigare nella zona del sito Domino in cui si effettuano le elaborazioni di pagamento dei clienti e di cancellare tutti i dati che si trovano più a valle nel codice rispetto al nome del database su cui lavora il daemon.

2 **Attacco di hacking remoto:** tutte le piattaforme sono sensibili a questo attacco che porta alla modifica dei contenuti. Si sfrutta inviando un URL artefatto che invia al al server una richiesta "EditDocument" invece della classica "OpenDocument" ottenedo così la possibilità di modificare i file.

3 **Attacco hacking:** tutte le piattaforme sono sensibili a questo baco che consente la modifica via Internet dei documenti. Aggiungendo domcfg.nsf/?open all'indirizzo Web un hacker riesce a capire cosa e come è modificabile un database remoto garantendosi così la possibilità di accedere in modalità scrittura ai file stessi.

>> Novell Web Server



La Novell (www.novel.com) offre soluzioni che permettono la trasformazione di un server NetWare in un server Internet/intranet. È un sistema completamente integrato con Netscape, di cui Novell è partner.
I rischi documentati sono i seguenti:

1 **Attacco Denial-of-Service:** le versioni NetWare 4.11 sono sensibili a un attacco TCP/UDP che porta al blocco totale del sistema. Utilizzando un modulo incluso nel server, il tcpip.nlm, si aprono dei varchi al sistema che consentono di attaccare i servizi echo e chargen. Sulla porta 7 (echo) viene effettuato un attacco DoS di tipo Ping of Death oppure Ping flooding. La prima consiste nell'invio di un PING con dimensioni superiori ai 65536 byte che il sistema non riesce ad interpretare e che quindi provoca un blocco, mentre la seconda consiste nella saturazione delle risorse con richieste continue di risposte a pacchetti PING. L'attacco sulla porta 19 invece ha come risultato la chiusura del servizio DNS della porta 53 a causa dell'arrivo di una stringa, generata appunto dal servizio chargen, con eccesso di caratteri.

2 **Attacco di overflow:** se si invia una grossa richiesta di tipo GET alla porta di amministrazione si riesce a provocare un buffer overflow che permette di eseguire codici non autorizzati. Questo bug è sfruttabile utilizzando il file nwtcp.c reperibile in rete.

CAT4R4TTA
cat4r4tta@hackerjournal.it

? Cgi-bin
Cartella presente nei vari spazi di hosting abilitata all'esecuzione di script CGI (Common Gateway Interface).

ENUMERAZIONE DELLE RISORSE DISPONIBILI SU UN SERVER

Cosa gira sul tuo

Il primo passo di un attacco consiste nello scoprire tutte le informazioni possibili su un PC: i servizi attivi, gli utenti registrati, i permessi. Ecco come si fa.

L'enumerazione è una fase dell'hacking spesso trascurata o poco analizzata, eppure è fondamentale nell'acquisizione d'informazioni utili per attacchi successivi. Il suo scopo è l'individuazione delle condivisioni, degli utenti registrati su un server e delle applicazioni installate in modo da avere un quadro completo del target per progettare delle sortite mirate senza andare alla cieca. Dei tool che utilizzeremo alcuni sono già presenti nei SO Windows, purché stiate utilizzando Win2000pro, XP Professional o, naturalmente, Windows 2000 server, altri sono di terze parti. I target sono i server Microsoft. Prima di cominciare però assicuratevi di disabilitare momentaneamente eventuali firewall software, alla presenza dei quali, queste tecniche non funzionano perché vengono bloccate le risposte in ingresso qualora non siano aperte le porte utilizzate.

>> Enumerazione su NetBios

La vera e propria "gola profonda" dei server NT/2000 è come sempre il NetBios. Infatti, nel momento in cui riusciamo ad effettuare una connessione nulla (anonima) con la seguente istruzione dalla console:

```
net use \\nome-server\IPC$
"" /user:""
```

possiamo interrogare il server target con net view \\nome-server; a questo punto il server ci restituisce l'elenco delle condivisioni della macchina (figura1). Al posto di nome-server potete usare il suo ip.

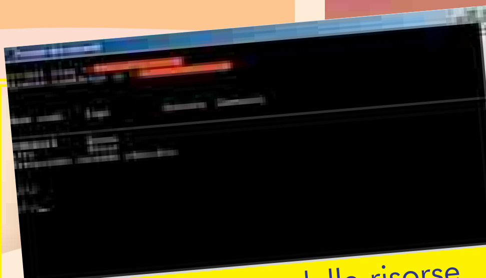


Figura 1. L'elenco delle risorse condivise dal server bersaglio.

Un'altra istruzione utile che può restituirci informazioni sui nomi netbios è la seguente:

```
nbtstat -A ip-server-target
```

Restituisce una tabella dei nomi NetBios simile a quella di figura 2. Il significato dei nomi sulla destra è specificato dal codice NetBios che si può trovare accanto. Ad esempio il nome del computer seguito dal codice 20 nella prima riga indica che la macchina WWW svolge un servizio di file server, il codice 00 presente nella seconda e terza riga invece indica rispettivamente il nome del computer e quello del dominio o del gruppo di lavoro (un elenco completo dei codici NetBios lo trovate su: http://jcifs.samba.org/src/docs/nbtcodes.html) ; alla fine viene fornito il MAC Address ossia l'indirizzo fisico della scheda di rete installata sulla macchina.



Figura 2. Il risultato del comando nbtstat, che fornisce informazioni sulle risorse condivise.

>> Strumenti utili

Oltre a queste informazioni il NetBios ne può fornire anche altre anche più interessanti però in questo caso è necessario ricorrere a strumenti non compresi nel SO ma facilmente disponibili in rete come ad esempio DumpAcl, tool visuale reperibile gratuitamente presso il sito della Somarsoft (http://www.somarsoft.com) . Sfruttando sempre le sessioni NB nulle, questo applicativo consente di risalire, oltre che all'elenco delle risorse condivise (file e stampanti), anche alla lista completa degli utenti e dei gruppi, alle chiavi di registro del sistema, ai servizi installati sulla macchina, le politiche di sicurezza utilizzate dall'amministratore e i diritti attribuiti a ogni gruppo. Tutte queste informazioni inoltre possono essere intabellate come volete (figura3).

Per evitare quindi che il vostro servizio NetBios si trasformi in una spia del nemico dovete seguire alcuni accorgimenti:

1 Qualora il servizio non vi serva all'esterno della rete, è preferibile chiudere completamente le porte che vanno da 135 139 con un firewall. Su Windows 2000 dovete chiudere anche la 445 del CIFS/SMB che è in grado di fornire le stesse informazioni allo stesso modo.

2 Se non avete un firewall, ma il servizio non vi serve potete semplicemente disabilitarlo. Per quanto riguarda Win2000 abbiamo già visto come si fa (HJ n.12 "Autenticazione di sistemi NT/2000"), per NT basta disabilitare il binding del WINS Client (TCP/IP) andando su Control Panel->Network->Cartella Bindings, selezionate Wins Client e cliccate su Disable (Figura 4).

3 Se il NetBios vi serve, allora non vi resta che disabilitare soltanto l'accesso anonimo. Per far questo su

COMPUTER

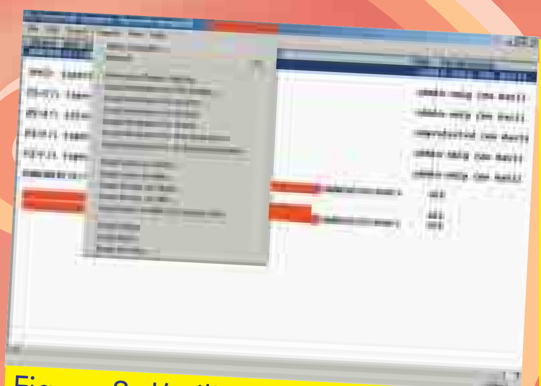
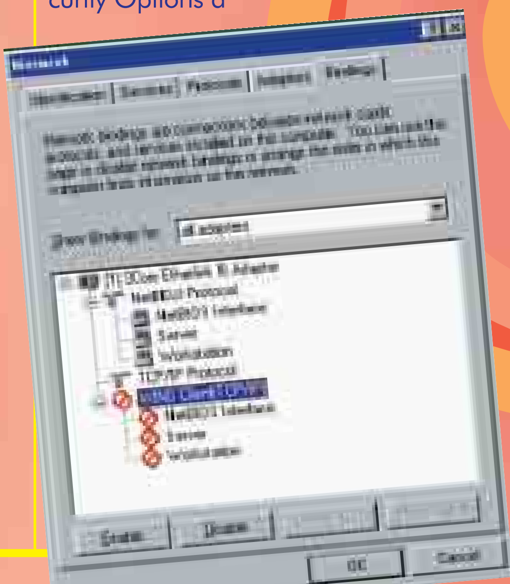


Figura 3. L'utility DumpAcl, che rivela ancor più dettagli sulle condivisioni, su utenti e gruppi, sulle policy di sicurezza e sui permessi attribuiti agli utenti.

NT dovete mettere le mani sul registro di configurazione per cui fatevi il segno della croce e aprite regedt32; portatevi su: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet \Control\Lsa; a questo punto aggiungete una chiave selezionando Edit->Add Value. Il ValueName di questa nuova chiave deve essere RestrictAnonymous il Data Type REG_WORD ed il Value 1. Chiudete il regedt32 e riavviate il computer per rendere effettive le modifiche. Per quanto riguarda Win2000 invece l'operazione è un po' più semplice poiché dovete soltanto andare sulle Local Security Settings, raggiungibili dall'MMC, poi su Security Options a

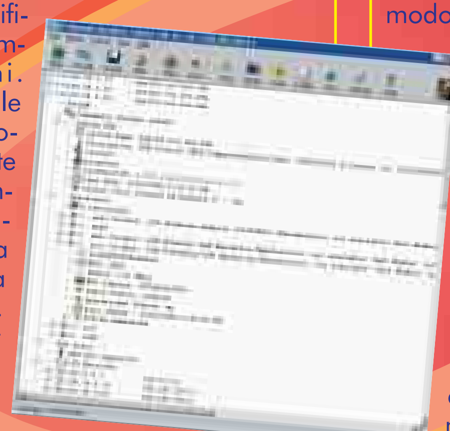


questo punto dalla finestra di sinistra selezionate Additional restrictions for anonymous connections e dal menù a tendina delle Local policy setting selezionate No access without explicit anonymous permission.

A questo punto dovreste essere al riparo dall'enumerazione che sfrutta NetBios ma, ahimè, non da altri tipi d'enumerazione.

>>Enumerazione su SNMP

L'SNMP (Simple Network Managment Protocol) è un protocollo che viene utilizzato per il controllo ed il monitoraggio di tutti i dispositivi di una rete. La comunicazione con tali dispositivi avviene attraverso le porte TCP e UDP 161 e 162. Dalla prima passano le richieste GET attraverso le quali un SNMP Manager da remoto richiede i dati del sistema, dalla seconda passano le richieste SET di modifica delle impostazioni. Entrambe le richieste sono corredate da un community name che fa un po' da password. Di default questo communituy name è 'public',



e raramente viene cambiato, per cui è molto comune trovare in rete dei server che attraverso un'interrogazione SNMP forniscono nell'ordine: interfacce di rete installate (schede), servizi attivi, nomi account degli utenti, cartelle condivise, stampanti condivise, tabelle di routing, servizi UDP e chi più ne ha più ne metta. Naturalmente per fare tutto ciò serve qualche tool: a tal proposito quello che secondo me si trova una spanna al di sopra degli altri è l'IP Network Browser



della Solarwinds (www.solarwinds.net). Questo tool è compreso in un pacchetto per la gestione e il monitoraggio di una rete; è a pagamento, però è possibile provarlo. Inoltre, se la cosa può interessarvi, viene utilizzato anche per recuperare informazioni di server non Microsoft e soprattutto di vari tipi di router.

Per far fronte alla vulnerabilità del servizio SNMP potete:

1 Rimuovere del tutto l'agente SNMP o disattivare il servizio SNMP nei Services del Pannello di Controllo.

2 Se non volete o non potete eliminare SNMP potete cambiare il community name sostituendo il public con uno personalizzato.

3 Se utilizzate SNMP ma soltanto per la rete interna potete fare in modo che le porte 161 e 162 TCP/Udp non siano accessibili dall'esterno (sempre con il firewall).

Le tecniche d'enumerazione fin qui descritte non sono le uniche. Ve ne sono altre che probabilmente tratteremo in altri articoli (enumerazione del registro, di Active Directory eccetera). Per adesso però vorrei soffermare la vostra attenzione sull'utilità dell'enumerazione e quindi sull'opportunità d'impedirla:

Enumerare un server consente di recuperare i nomi degli utenti, informazione che riduce del 50% il tempo di un attacco a forza bruta. Inoltre la password può anche essere uguale al nome utente (capita ancora!).

Consente di conoscere i servizi attivi nel server con un rischio da parte dell'intruso equivalente a quello di un portscan, ma con un risultato molto migliore: immaginate cosa può significare essere informato su sistemi di Intrusion Detection, oppure avere un elenco completo di servizi per la ricerca di vulnerabilità.

Roberto "dec0der" Enea

INTRODUZIONE AL PERL, LINGUAGGIO COMPLICATO MA MOLTO VERSATILE

PERL: il paradiso degli hacker



Il Perl è uno di quei linguaggi di programmazione che permette di amministrare con semplicità un sistema informatico... il proprio o quello di altri.

Il Perl (Practical Extraction and Report Language) è un formidabile linguaggio di programmazione nato nel 1987 dalla mente di Larry Wall. Lo scopo di questo linguaggio era quello di aiutare un complesso sistema multipiattaforma, di cui Larry era appunto il gestore. L'obiettivo consisteva nel creare un linguaggio che permettesse il parsing dei file di configurazione e di log nel modo più semplice possibile. A distanza di tempo, il Perl si è evoluto e attualmente è uno dei linguaggi di programmazione più usati nella scrittura di procedure CGI da implementare su Web Server e per lo sviluppo di programmi per la manutenzione delle attività di un server. La sintassi del Perl è molto pulita e si nota fin da subito la somiglianza con due linguaggi di programmazione noti a qualsiasi utente Unix, il C e gli script di shell. Inoltre, Perl è un linguaggio interpretato e questo comporta dei vantaggi, come la totale portabilità e la disponibilità del codice sorgente.

>> L'ambiente di sviluppo

Reperire e installare tutto il software necessario per potere cominciare a creare i primi script in Perl non è affatto difficile. Potete scaricare l'interprete per la vostra piattaforma da www.cpan.org.
In questo sito è anche possibile reperire abbondante documentazione e numerosi esempi di script. Gli utenti Linux con molta probabilità non dovranno preoccuparsi di effettuare il download dell'interprete in quanto questo è già preinstallato nelle maggiori distribuzioni. Comunque per essere certi di avere già installato l'interprete digitate dalla shell il seguente comando:

```
$ whereis perl
```

Se da questo otterrete un percorso del tipo /usr/bin/perl, vorrà dire che questo è il Path in cui si trova il vostro interprete Perl. Adesso invece passiamo all'installazione sotto Windows. Una distribuzione di Perl per questo sistema operativo è ActivePerl e sul sito www.activestate.com è possibile scaricare direttamente il file di installazione e la copiosa documentazione che viene fornita col pacchetto sarà senza dubbio di grande aiuto per i novizi. Per installare l'interprete sotto Windows, occorre scompattare il file appena scaricato all'interno di una directory e lanciare l'eseguibile installer.bat. Comparirà a questo punto il prompt del dos che vi chiederà dove installare l'interprete. Dopo avere digitato il path che preferire per la vostra installazione (es. C:\ perl) si procederà con l'installazione vera e propria. Per una installazione di default digitate sempre 'y' ad ogni domanda che vi porrà il file di installazione ed il gioco è fatto! L'interprete Perl si troverà nella sottodirectory bin di Perl, col nome di perl.exe.

CGI Common Gateway Interface. È l'interfaccia tra le pagine Web e le procedure che elaborano i dati passati da tali pagine e forniscono in output dati in formato html.

>> Da dove comincio

Cominceremo con la codifica di uno script semplice. Da questo momento consideriamo che il vostro interprete sia installato in C:\Perl\bin per la versione Windows e /usr/bin/perl per la versione Linux.



Larry Wall, il padre del linguaggio Perl. Da notare l'aria da Nerd anni 70'...

```
#!/usr/bin/perl
#!c:/perl/bin/perl.exe
print " Un saluto da Hacker
Journal\n ";
```

Salvando queste poche righe di codice col nome ciao.pl otterremo il nostro primo script in Perl che visualizza sul monitor la stringa preceduta dal comando print. Nello script precedente abbiamo anche inserito il commento speciale introdotto dai simboli "#!" che indica al sistema dove trovare l'interprete Perl sia su Linux che su Windows. Da questo momento in poi eviteremo di aggiun-

gere il commento speciale all'inizio dello script, ricordando ai lettori di inserire quello necessario per il proprio sistema operativo.

Adesso facciamo un piccolo esempio che ci premetta di potere utilizzare una semplice variabile:



Il sito www.cpan.org da dove è possibile prelevare l'interprete Perl per ogni tipo di piattaforma, ma anche documentazione varia e parecchi script di esempio.

```
$a= "Un saluto da Hacker
Journal\n"
print "$a\n";
```

Come potete vedere prima abbiamo attribuito un valore stringa alla variabile $a e poi facciamo stampare la variabile sul monitor. Il risultato sarà uguale a quello dello script precedente, ma il tutto verrà semplificato grazie all'utilizzo delle variabili. I lettori più attenti avranno sicuramente notato come non sia necessario dovere dichiarare il tipo di variabile (così come con Python). Con la stessa semplicità è anche possibile gestire dati di tipo numerico grazie agli operatori numerici. Esistono diversi tipi di operatori numerici, vediamo i più comuni:

Operatori aritmetici: +, -, *, / , %
Operatori di confronto: < , > , <= , >= , = = , ! =
Operatori incremento e decremento: $a++, $a—, ++$a, —$a

Il linguaggio Perl gestisce inoltre con estrema naturalezza le operazione tra valori numerici e stringhe. Infatti se usiamo un valore numerico in una stringa, questo verrà convertito in una stringa, mentre se usiamo una stringa in un contesto numerico, la nostra stringa sarà considerata un valore numerico dall'interprete.

Vediamo un esempio:

```
$a = "08 ". "gennaio ".
"2000";
print "$a\n";
```

In questo caso mediante l'operatore di addizione stringhe (il punto), i valori numerici saranno considerati stringhe e quindi come output avremo 08 gennaio 2000, mentre se utilizzassimo questo script:

```
$a = "08"+ "gennaio
"+"2000";
print "$a\n";
```

noteremo che l'operatore numerico addizione costringe l'interprete a considerare la stringa gennaio come un numero, nel nostro caso uguale a 0, e quindi l'output sarà 2.008.
Proviamo adesso a creare un programmino che ci permetta un minimo di interazione. L'istruzione che ci consente di inserire output da tastiera è <STDIN>, ovvero standard input, racchiuso tra parentesi angolate. Eccovi un esempio:

```
print " Inserisci il tuo
nome \n";
$nome = <STDIN>;
print " Inserisci il tuo
cognome\n";
$cognome = <STDIN>;
chomp ($nome);
chomp ($cognome);
print "Il tuo nome è $nome,
mentre il tuo cognome è
$cognome\n";
In questo semplice script
notiamo che l'istruzione
"chomp ( $variabile)"
rimuove il carattere di
escare, ottenuto dalla
pressione del tasto invio,
dalle stringhe.
```

>> Strutture dati: gli array

Oltre alle variabili scalari analizzate fino a questo momento, il Perl ci permette di utilizzare un altro tipo di variabili: gli array. Un array è una sequenza ordinata di valori scalari. È possibile interagire con ogni singolo valore racchiuso nell'array. Vediamo come generarne uno:

```
@amici = ('Marco','
Claudio',
'Lina','Paolo','TAIS+');
print "I miei amici veri
sono $amici[0], $amici[1],
$amici[3]\n";
print "mentre $amici[2]
$amici[4] sono piu' che
amici…\n";
```

Eccovi l'output:

```
I miei amici veri sono
Marco, Claudio, Paolo
Mentre Lina TAIS+ sono più
che amici…
```

Bene, con lo script appena realizzato potete vedere come ogni singolo valore scalare contenuto all'interno dell'array possa essere utilizzato in modo del tutto naturale. Per rendere ulteriormente flessibile l'utilizzo degli array, il Perl mette a disposizione alcuni operatori speciali sulle strutture dati. Vediamo qualche esempio:



Utilizzando un semplice editor di testo come Edit Plus che supporta la sintassi del Perl, saremo agevolati nella codifica dei nostri script.

Push e pop
Questi operatori agiscono sull'ultimo elemento dell'array, e precisamente push aggiunge valori in coda alla lista mentre pop toglie l'ultimo elemento dall'array.

```
@numeri = (25,42,63,69);
push (@numeri, 52);
```

In questo caso abbiamo aggiunto l'elemento 52 all'array @numeri, mentre:

```
@numeri = (25,42,63,69);
pop (@numeri);
```

Adesso l'ultimo elemento sarà cancellato dalla pila di dati.
Shift e unshift

INTRODUZIONE AL PERL, LINGUAGGIO COMPLICATO MA MOLTO VERSATILE

Questi operatori agiscono invece sul primo elemento della lista, infatti mediante l'operatore shift è possibile togliere il primo elemento dalla lista mentre con unshift è possibile aggiungere nuovi valori in testa all'array.

```
@numeri = (25,42,63,69);
shift (@numeri);
```

toglierà l'elemento 25 dalla lista mentre

```
@numeri = (25,42,63,69);
unshift(@numeri, 63,32);
```

aggiungerà gli elementi numerici 63 e 32 in testa all'array.

Sort e reverse
Con questi operatori è possibile riordinare gli elementi delle liste in modo crescente o decrescente. Nel caso in cui gli elementi dell'array fossero delle stringhe verranno sistemate in ordine alfabetico.

>> Istruzioni Condizianali

Grazie alle istruzioni condizionali è possibile realizzare script che ci permettano di eseguire gruppi di istruzioni differenti al verificarsi di una determinata condizione. Le istruzioni condizionali (o decisionali) in Perl sono if, else e elsif. Vediamo subito un esempio per capire come implementare delle istruzioni di condizionamento all'interno dei nostri script:

```
print " Inserire qui la
password\n";
$password= <STDIN>;
chomp ($password);
if ($password == 1234 ) {
print " Complimenti pas-
sword corretta\n" }
elsif ( $password == 1235 )
{
print "Hai sbagliato una
cifra\n" }
else {
print " Mi spiace, password
errata\n" }
```

Abbiamo realizzato uno script un po' banale ma utile a far comprendere l'utilizzo delle differenti istruzioni decisionali.

Script Programma che viene eseguito da un interprete, e non dal sistema operativo stesso. Gli script più comuni sono gli script di shell, i JavaScript (che vengono eseguiti dal browser) e, in ambiente Macintosh, gli AppleScript.

>> Cicli e iterazioni

Le istruzioni iterate vengono eseguite ripetutamente all'interno di un blocco fino al raggiungimento della condizione. Nel linguaggio Perl le principali istruzioni iterative sono while e for. Vediamo un esempio:

```
$a=2;
while ($a<10) {
 $a++;
}
print "$a\n";
```

Questo script controlla se il valore di $a sia minore di 10, e se questa istruzione risulta vera incrementa ripetutamente il valore di $a fino a quando non raggiunge il valore 10. L'output di questo script sarà quindi 10.
Sebbene anche il costrutto for faccia parte delle istruzioni iterative la sua sintassi è ben diversa da quella dell'istruzione while:

```
for ($a=0; $a <10; $a++) {
print "Un saluto da Hacker
Journal\n";
}
```

LE PERLE DI PERL

www.perl.com
Sito specifico su Perl del circuito di O'Reily

www.perldoc.com
Un mare di documentazione su Perl

www.perlmonks.org
Comunità di utenti Perl, con trucchi, consigli e spezzoni di codice

www.scriptitalia.net/script/linguaggio.php?risorsa=tutorial&linguaggio=perl
Tutorial in italiano su Perl

www.dei.unipd.it/~tigre/b/PerlTutorial/
Traduzione italiana di un noto tutorial Perl

Lanciando questo script noterete che la stringa di saluto sarà ripetuta per 10 volte, in quanto la variabile $a verrà sempre incrementata di 1 ma si fermerà non appena raggiunge il valore 10.

>> Manipolare i file

Fino a questo momento ci siamo limitati a descrivere brevemente le nozioni base che il linguaggio ci offre. All'inizio dell'articolo abbiamo accennato al fatto che il punto di forza di questo linguaggio di programmazione consiste proprio nella manipolazione dei file. Come sempre, niente è più esplicativo di un esempio commentato:

```
1. $uno
='C:\esempi\uno.txt';
2. $due ='C:\esempi\due.txt;
3. open (a, "<$uno") or die
"Non posso aprire il file
specificato";
4. open (b, ">$due") or die
"Non posso aprire il file
specificato";
5. while ($riga=<a>) {
6. print b $riga;
 }
7. close (a);
8. close (b);
```

Per prima cosa dobbiamo creare due file all'interno della cartella appositamente creata (C:\esempi) e nominarli rispettivamente uno.txt e due.txt. Scriviamo ciò che vogliamo nel file uno.txt e lasciamo l'altro vuoto. I punti 1 e 2 del nostro script attribuiscono rispettivamente le variabili $uno e $due ai file appena creati. Con le istruzione 3 e 4 apriamo il file valorizzato in $uno che identificheremo con la lettera 'a' ed il file $due che è identificato dalla lettera 'b'. Ma mentre il file 'a' è di sola lettura (<$uno) , il file b è di sola scrittura (>$due). Con l'istruzione while stampiamo tutte le stringhe contenute in $uno nel file $due. Infine con le istruzioni 7 ed 8 chiudiamo i nostri file. Adesso lanciate lo script e aprite i file di testo: il contenuto di 'a' è stato copiato in 'b'!

Studiate, leggete il codice scritto da altri e contribuite a migliorarlo...

Antonino Benfante

come ti MASTERIZZO il Service Pack

Quando si reinstalla Windows (e capita più spesso di quanto dovrebbe), una delle cose più noiose è andare alla ricerca dei Service Pack e delle patch di aggiornamento. Non sarebbe più comodo usare un unico CD con un sistema già aggiornato?

CREARE UN CD DI INSTALLAZIONE DI WINDOWS CON SERVICE PACK INCLUSI

Quante volte vi è capitato di reinstallare il sistema operativo con i relativi service pack? E quanto tempo avete passato davanti al computer per reinstallare il tutto? C'è un modo per risparmiare tempo e soprattutto per rendere il sistema operativo più leggero.
Prima di iniziare premetto che questa procedura serve solo per gli utenti che utilizzano Windows 2000 & XP, ed è consentita solo ed esclusivamente a coloro che vogliono creare delle copie di backup e sicurezza della propria licenza originale tutti gli altri usi sono illegali.

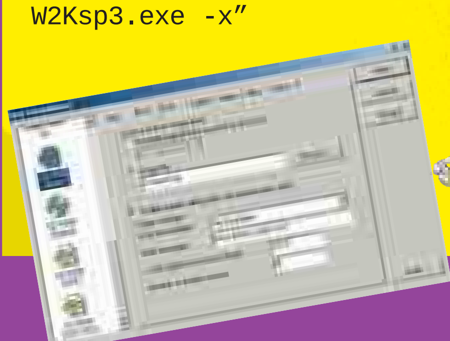
>> Preparazione dei file

Ecco a voi la procedura passo passo:

1 La prima cosa da fare è scaricare l'ultimo Service Pack, dalla Microsoft, e salvarlo ad esempio in C:\sp3\W2Ksp3.exe;

2 Andate nel prompt di MS-DOS posizionatevi nella cartella "c:\sp3>" e scrivete:

```
W2Ksp3.exe -x"
```



Partirà automaticamente una finestra che vi chiederà dove decomprimere il file "W2Ksp3.exe", io ho scelto la stessa cartella d'origine.

3 una volta terminata la procedura di estrazione passiamo alla copia del nostro CD di installazione di Windows sull'hard disk in una cartella, per esempio c:\W2k.

4 Posizioniamoci con il prompt di MS-DOS all'interno della cartella sp3i386update è digitiamo

```
update –s:c:\win2000
```

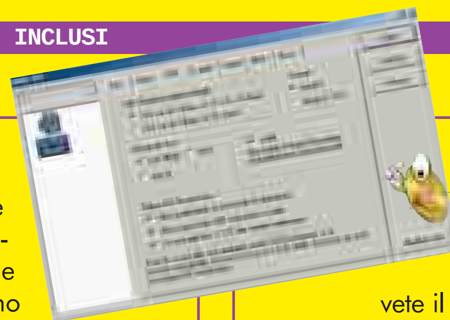
Premiamo invio, e adesso abbiamo la nostra bella copia di windows già aggiornata con il Service Pack.

5 Scaricate il file boot.img da http://digilander.libero.it/issues75/boot.img e salvatelo, per esempio in c:\;

>> Masterizzazione

Per masterizzare il CD, è meglio usare Nero (ma non in modalità Wizard, per cui andate in modalità normale dopo averlo avviato.

6 Selezionare "CD-ROM (boot)".



7 Nella sezione "boot":
•Selezionate "File immagine" e scrivete il percorso c:\boot.img.
•Selezionate Abilita impostazioni avanzate (solo per utilizzatori esperti!) andate sulla voce Tipo di emulazione e selezionare Nessuna emulazione.
•Su Carica segmento del settore (hex!): scrivete 07C0.
•Su Numero di segmenti caricati: scrivete 4.

8 Nella sezione ISO controllate che siano evidenziati i seguenti valori:
•ISO Level 1
•Mode 1
•ISO 9660
•Joliet

9 Infine andate nella sezione Scrivi, Chiudi CD, e mettete come metodo di scrittura Disc-At-Once e fate clic su New.

10 Trascinate i file della cartella Win2000 con il metodo DRAG & DROP e, una volta terminato, fate partire la masterizzazione cliccando su Write Cd. Ecco fatto il vostro CD bootabile con Service Pack aggiornato.

KoRn issues75@libero.it

